

NATを使用したWorkgroup Bridge(WGB)有線クライアントの設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[バックグラウンド情報](#)

[ネットワーク図](#)

[設定](#)

[ワイヤレス LAN コントローラ](#)

[ワークグループブリッジ](#)

[ルータ](#)

[ワイヤレス LAN コントローラ](#)

[ワークグループブリッジ](#)

[ルータ](#)

はじめに

このドキュメントでは、Workgroup Bridge経由でネットワークにアクセスするための、Network Access Translation (NAT ; ネットワークアクセス変換) の背後にある有線クライアントの設定について説明します。

前提条件

要件

次の項目に関する知識があることを推奨しています。

- 9800ワイヤレスLANコントローラ(WLC)の概念と設定
- Workgroup Bridge(WGB)の概念と設定
- ネットワークアクセスコントロール(NAT)の概念と設定
- スイッチングの概念と設定

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- 9800-CL WLC Cisco IOS® XE 26.1.1
- 1821ルータバージョン26.1.1に統合されたWGB WP-WIFI6-B
- Catalyst IR1821高耐久性ルータ、Cisco IOS 17.15.4
- 9300スイッチ、Cisco IOS 17.15.4

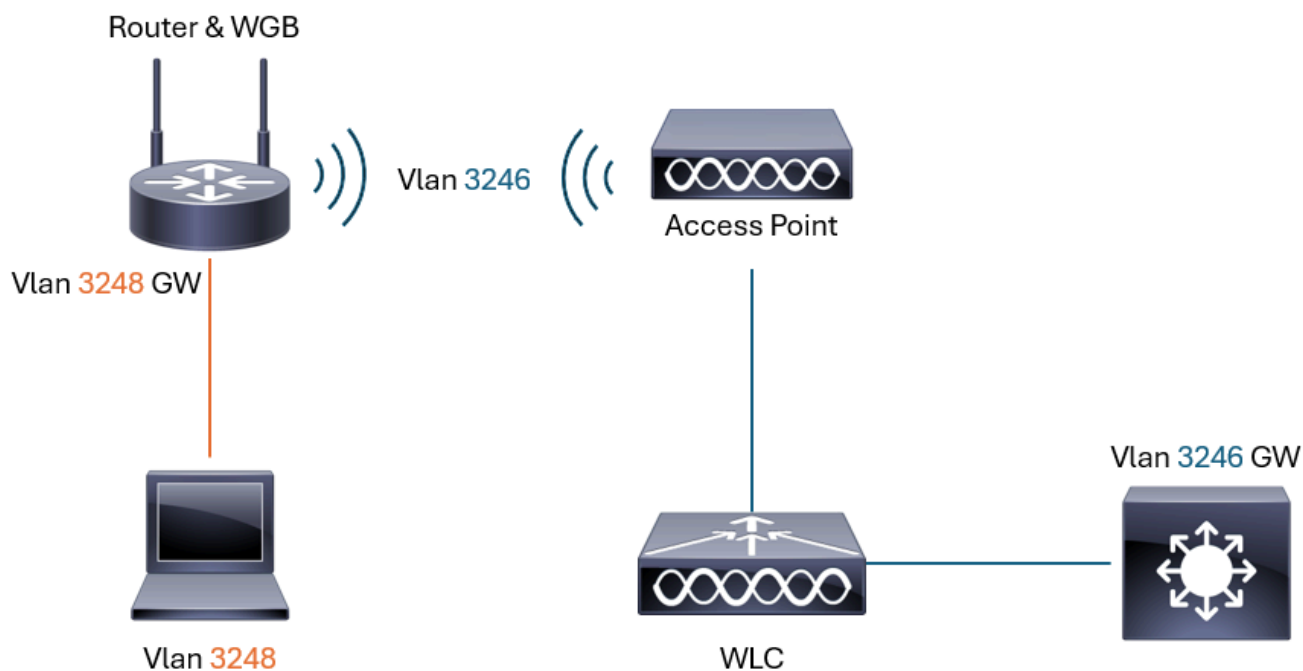
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

バックグラウンド情報

WGB実装には、WGBの背後の有線クライアントをWGBとは異なるvLANに配置する必要があり、同時にvLANがWGB、WLC、またはWLCの背後のネットワークデバイスに存在しない場合があります。

このシナリオでは、NATを使用すると、有線クライアントがWLCの背後にあるネットワーク（アプリケーション、インターネット、サーバなど）と通信するために必要な設定と柔軟性が提供されます。

ネットワーク図



トポロジ

設定

ワイヤレス LAN コントローラ

このセクションでは、WGBが接続するサービスセット識別子(SSID)をブロードキャストするためのWLAN、WLANポリシープロファイル、およびポリシータグの基本設定について説明します。



注意：実稼働環境でこれらのパラメータの設定を変更すると、ワイヤレスクライアントの接続が解除される可能性があります。

ステップ 1：SSID を設定します。

ステップ 1.1：Configuration > Tags & Profiles > WLANsの順に選択します。[Add] をクリックします。ProfileとSSIDの名前を入力します。[APPLY] をクリックします。

GUI：

Configuration > Tags & Profiles > WLANs

+ Add × Delete Clone Enable WLAN Disable WLAN

Add WLAN

General Security Advanced

Profile Name* WGB

SSID* WGB

WLAN ID* 6

Status ENABLED ☒

Broadcast SSID ENABLED ☒

> Wi-Fi 6E Compatibility 1/2 requirements met

> Wi-Fi 7 Compatibility 0/3 requirements met 0/3 bands enabled

Radio Policy ⓘ

Show slot configuration

6 GHz
Status DISABLED ☐

5 GHz
Status ENABLED ☒

2.4 GHz
Status DISABLED ☐

802.11b/g Policy 802.11b/g ▼

Cancel Apply to Device

Wlanの設定

CLI :

```
config t
wlan WGB 6 WGB
radio policy dot11 5ghz
no shutdown
```

ステップ 1.2 : SSIDセキュリティパラメータを設定します。PSKを選択し、PSKパスワードを入力して、Applyをクリックします。

GUI :

Edit WLAN

Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

General
Security
Advanced
Add To Policy Tags

Layer2
Layer3
AAA

☒ WPA + WPA2
☐ WPA2 + WPA3
☐ WPA3
☐ Static WEP
☐ None

MAC Filtering
☐

Lobby Admin Access
☐

WPA Parameters

WPA Policy
☐
WPA2 Policy
☒

GTK Randomize
☐
OSEN Policy
☐

WPA2 Encryption

AES(CCMP128)
☒
CCMP256
☐

GCMP128
☐
GCMP256
☐

Protected Management Frame

PMF
Disabled

Fast Transition

Status
Disabled

Over the DS
☐

Reassociation Timeout *
20

Auth Key Mgmt (AKM)

802.1X
☐
FT + 802.1X
☐

802.1X-SHA256
☐
CCKM
☐

PSK
☒
FT + PSK
☐

PSK-SHA256
☐
Easy-PSK
☐

PSK Format
ASCII

PSK Type
Unencrypted

Pre-Shared Key*

Cancel
Update & Apply to Device

WLAN セキュリティ

CLI :

```

config t
wlan WGB 6 WGB
shutdown
no security ft adaptive
security wpa psk set-key ascii 0 12345678
no security wpa akm dot1x
security wpa akm psk
no shutdown

```

ステップ 1.3 : SSIDでAironetIEを設定します。Advancedタブに移動し、CCX Aironet IEを有効

にして、Applyをクリックします。

GUI :

Edit WLAN

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

GeneralSecurityAdvancedAdd To Policy Tags

Coverage Hole Detection☒

CCX Aironet IE☒

Advertise AP Name☐

P2P Blocking Action

Disabled

Multicast Buffer

DISABLED

Media Stream Multicast-direct☐

11ac MU-MIMO☒

Wi-Fi to Cellular Steering☐

Wi-Fi Alliance Agile Multiband

DISABLED

Fastlane+ (ASR) ☒

Deny LAA (RCM) clients☐

6 GHz Client Steering☐

Latency Measurements Announcements☐

Universal Admin☐

OKC☒

Load Balance☐

Band Select☐

IP Source Guard☐

WMM Policy

Allowed

mDNS Mode

Bridging

Off Channel Scanning Defer

Defer Priority

☐0☐1☐2

☐3☐4☒5

☒6☐7

Scan Defer Time

100

Assisted Roaming (11k)

Prediction Optimization☐

Max Client Connections

Per WLAN

n

Cancel

Update & Apply to Device

Aironet IE

CLI :

<#root>

```
config t
wlan WGB 6 WGB
shutdown
ccx aironet-iesupport
no shutdown
```

ステップ 2 WLANポリシープロファイルを設定します。

ステップ 2.1 : Configuration > Tags & Profiles > WLANsの順に選択します。[Add] をクリックします。名前を入力します。Enable the StatusおよびPassive Clientとして設定します。次に [Apply] をクリックします。

GUI :

Configuration > Tags & Profiles > Policy

+ Add × Delete Clone

Add Policy Profile

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

General Access Policies QOS and AVC Mobility Advanced

Name* PolicyWGB

Description Enter Description

Status ENABLED

Passive Client ENABLED

IP MAC Binding ENABLED

Encrypted Traffic Analytics DISABLED

CTS Policy

Inline Tagging ☐

SGACL Enforcement ☐

Default SGT 2-65519

WLAN Switching Policy

Central Switching ENABLED

Central Authentication ENABLED

Central DHCP ENABLED

Flex NAT/PAT DISABLED

Cancel Apply to Device

WLANポリシー

CLI :

<#root>

```
config t
wireless profile policy PolicyWGB
passive-client
no shutdown
```

ステップ 2.2 : Access Policiesに移動します。VLAN/VLAN Groupをクリックし、WGB vLANを選択します。

GUI :

Edit Policy Profile

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

General

Access Policies

QOS and AVC

Mobility

Advanced

RADIUS Profiling☐

HTTP TLV Caching☐

DHCP TLV Caching☐

WLAN Local Profiling

Global State of Device ClassificationDisabled ⓘ

Local Subscriber Policy NameSearch or Select ▼ ⓘ

VLAN

VLAN/VLAN GroupVLAN3246 × ▼ ⓘ

Multicast VLANEnter Multicast VLAN

Note : Selecting a VLAN Group is a valid config only for Central Switching SSIDs. Do not use with SSIDs enabled for Flex Local Switching

WLAN ACL

IPv4 ACLSearch or Select ▼ ⓘ

IPv6 ACLSearch or Select ▼ ⓘ

URL Filters ⓘ

Pre AuthSearch or Select ▼ ⓘ

Post AuthSearch or Select ▼ ⓘ

↶ Cancel

📄 Update & Apply to Device

Vlanの設定

CLI :

```
conf t
wireless profile policy PolicyWGB
shutdown
vlan VLAN3246
no shutdown
```

ステップ 3 ポリシータグを設定し、WGBの接続先であるアクセスポイント(AP)に適用します。

ステップ 3.1 : Configuration > Tags & Profiles > Tagsの順に移動します。Policyをクリックし、次にAddをクリックする。Nameを入力し、Addをクリックします。SSIDとPolicy Profileを選択します。[APPLY] をクリックします。

GUI :

Configuration > Tags & Profiles > Tags

Policy Site RF AP

+ Add × Delete Clone

Add Policy Tag

Name* WGBTag

Description Enter Description

WLAN-POLICY Maps : 1

+ Add × Delete

☐	WLAN Profile	Policy Profile
☐	WGB	PolicyWGB

1 50 items per page 1 - 1 of 1 Items

Map WLAN and Policy

Cancel Apply to Device

TAG

CLI :

<#root>

```
config t
wireless tag policy WGBTag
wlan WGB policy PolicyWGB
```



注：必ず、SSIDをブロードキャストするすべてのアクセスポイントのポリシータグに適用してください。

ワークグループ ブリッジ

このセクションでは、WGBの設定について説明します。この設定により、WGBがネットワークに接続し、vLAN3246を介して接続できるようになります。

CLI :

```
configure ap hostname WGB1
configure ap address ipv4 static 10.10.246.4 255.255.255.0 10.10.246.1
configure ap management add username admin password P0ssw0rd123! secret P0ssw0rd123!
configure ssid-profile WGB ssid WGB authentication psk 12345678 key-management wpa2
configure dot11Radio 1 mode wgb ssid-profile WGB
configure dot11Radio 1 enable
```

ルータ

このセクションでは、vLAN3248の有線クライアントとvLAN3246の間の接続を可能にするためにNATを設定する方法について説明します。

vLAN3248はルータ内にのみ存在し、WLCの背後にあるネットワーク側への接続は一切行われません。

ルータはNATを実行して、vLAN3248の有線クライアントのトラフィックを、WGBを介してvLAN3246のWLCの背後にあるネットワーク側に転送します。



注:WGBの背後のルータに接続されている有線クライアントの場合、vLANからの接続を確保するためにサポートされている設定はNATのみです。Inter-vLANルーティングはサポートされていません。

ステップ 1 : vLAN 3246およびvLAN 3248をレイヤ2レベルで設定します。

```
conf t
vlan 3246
exit
vlan 3248
end
```

ステップ 2ルータからWGBのポートを設定します。

```
conf t
interface Wlan-GigabitEthernet 0/1/4
switchport trunk native vlan 3246
switchport trunk allowed vlan 3246
switchport mode trunk
```

ステップ 3WGB vLANと有線クライアントvLANのスイッチ仮想インターフェイス(SVI)を設定します。

ステップ 3.1 : WGB SVI設定。IPアドレス10.10.246.1は、WLCの背後にあるレイヤ3スイッチで設定されたvLAN 3246のゲートウェイです。ルータ内のこのSVIは、次に使用可能なIPアドレスを使用しています。

```
config t
interface Vlan3246
ip address 10.10.246.2 255.255.255.0
```

ステップ 3.2 : 有線クライアントインターフェイスのvLAN設定ルータの有線クライアントはvLAN 3248を使用するこのSVIは有線クライアントのゲートウェイです。有線クライアントはこのルータにしか存在しないからです。このSVIに一意的MACアドレスを設定します。

```
config t
interface Vlan3248
mac-address 6c13.d53f.aabb
ip address 10.10.248.1 255.255.255.0
```



注意:SVIごとに一意のMACアドレスを設定してください。ルータはデフォルトですべてのSVIに同じMACアドレスを使用するため、この実装では競合が発生する可能性があります。

ステップ 4 アクセスリスト(ACL)を設定し、有線クライアントのネットワークを許可します。

```
config t
ip access-list extended NATACL
10 permit ip 10.10.248.0 0.0.0.255 any
```

ステップ 5 ACLとWGBインターフェイスに一致するルートマップを設定します。

```
conf t
route-map WGBACL permit 10
match ip address NATACL
match interface Vlan3246
```

ステップ 6 NAT を設定します。

ステップ 6.1 : SVIでNATを設定します。SVI 3248はNAT内部、3246はNAT外部です。

```
config t
interface Vlan3248
ip nat inside
exit
interface Vlan3246
ip nat outside
```

ステップ 6.2 : ルータでNATを設定します。送信元としてルートマップを使用します。この設定では、vLAN3248上の有線クライアントがWLCの背後にあるvLAN3246のネットワークに接続できます。

```
config t
ip nat inside source route-map WGBACL interface Vlan3246 overload
```

ステップ6.3このステップはオプションです。vLAN3246のWLCの背後にあるデバイスからvLAN3248のWGBの背後にあるデバイスにアクセスする必要がある場合は、NATを使用して設定できます。

例として、示されている設定は、vLAN3246のWLCの背後にあるデバイスからリモートデスクトッププロトコル(RDP)を介して、ルータの背後にあるデバイスとIPアドレス10.10.248.10のWGBへのアクセスを設定する方法を示しています。

vLAN 3248では、ルータの背後にあるデバイスのアクセス対象 (SSH、Telenet、RDP、HTTPなど) に応じて、任意のポートを使用できます。

RDPを使用して、vLAN3246内のデバイスから10.10.248.10デバイスにアクセスし、RDP接続がルータ(10.10.246.2)内の3246 vLANのSVIに対して行われるようにするには、このドキュメントの「[確認](#)」セクションを確認してください。

```
config t
ip nat inside source static tcp 10.10.248.10 3389 interface Vlan3246 3389
```

ステップ 7ルータのvLAN 3248に有線クライアントポートを設定します。

```
config t
interface GigabitEthernet0/1/0
switchport mode access
switchport access vlan 3248
```



注：この設定では、固定IPアドレスを持つvLAN 3248の有線クライアントを使用します。DHCPが必要な場合は、ルータで設定できます。

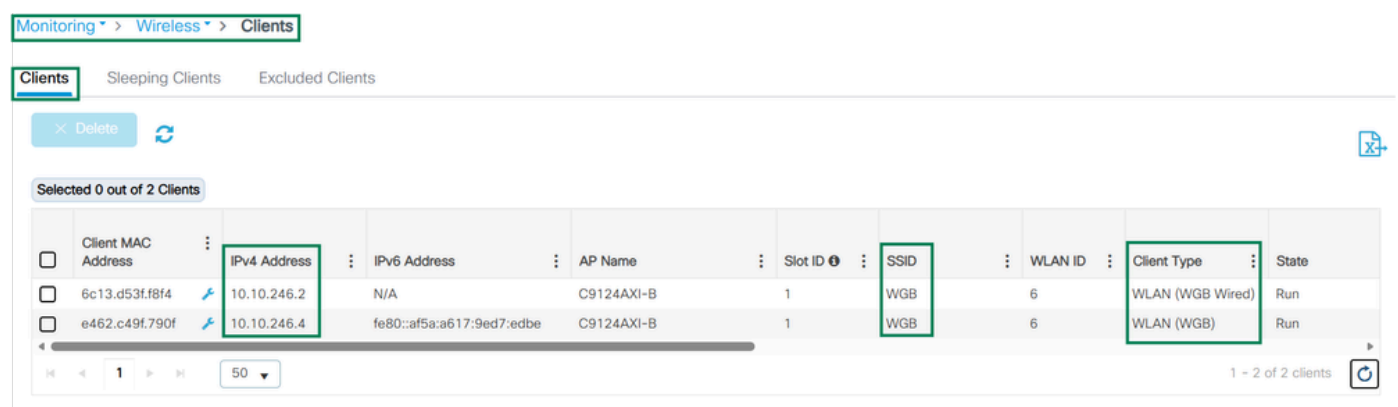
確認

有線クライアントとしてリストされているvLAN 3246のWGBとSVIの接続を確認します。また、vLAN 3248上の有線クライアントのネットワークへの接続を確認し、WLCの背後にあるvLAN 3246のゲートウェイにpingを送信します。

ワイヤレス LAN コントローラ

WLCから、ルータに設定されているvLAN 3246のWGBとSVIがワイヤレスクライアントリストに表示されていることを確認します。

GUI :



WGBおよびWGBクライアント

CLI :

<#root>

9800L#

show wireless client summary

Number of Clients: 2

MAC Address	AP Name	Type	ID	State	Protocol	Method	Role
6c13.d53f.f8f4	C9124AXI-B	WLAN	6	Run	11ac	None	Local
e462.c49f.790f	C9124AXI-B	WLAN	6	Run	11ac	None	Local

9800L#

show wireless client summary detail

Number of Clients: 2

MAC Address	SSID	AP Name	State	IP Address	VLAN	BSSID	Auth Method	Protocol	Channel
6c13.d53f.f8f4	WGB	C9124AXI-B	Run	10.10.246.2	3246	5c64.f171.6eae	[PSK]	11ac	36
e462.c49f.790f	WGB	C9124AXI-B	Run	10.10.246.4	3246	5c64.f171.6eae	[PSK]	11ac	36

9800L#

show wireless wgb summary

Number of WGBs: 1

MAC Address	AP Name	WLAN	State	Clients
e462.c49f.790f	C9124AXI-B	6	Run	1

ワークグループ ブリッジ

WGBがSSIDに接続されていることが示されていることを確認します。

<#root>

WGB#

show wgb dot11 associations

```

Uplink Radio ID : 1
Uplink Radio MAC : E4:62:C4:9F:79:0F
SSID Name : WGB
Connected Duration : 0 hours, 7 minutes, 9 seconds
Parent AP Name : C9124AXI-B
Parent AP MAC : 5C:64:F1:71:6E:AE
Uplink State : CONNECTED
Auth Type : PSK
Key management Type : WPA2
Dot11 type : 11ac
Channel : 36
Bandwidth : 20 MHz
Current Datarate : 104 Mbps
Max Datarate : 286 Mbps
RSSI : 41
IP : 10.10.246.4/24
Default Gateway : 10.10.246.1
IPV6 : ::/128
Assoc timeout : 5000 Msec
Auth timeout : 5000 Msec
Dhcp timeout : 60 Sec
Country-code : US

```

WGBブリッジテーブルにvLAN 3246のSVIが表示されていることを確認します。

<#root>

WGB#

show wgb bridge

```

***Client ip table entries***
mac vap port vlan_id seen_ip confirm_ago fast_brg
6C:13:D5:3F:F8:F4 0 wired0 0 10.10.246.2 28.112000 true
5C:64:F1:71:6E:AF 0 wbridge1 0 0.0.0.0 1064.320000 true

```

ルータ

ルータから、vLAN3248からvLAN3246のWLCの背後のネットワークに到達可能であることを確認し、これが成功します。

```
<#root>
```

```
Router#
```

```
ping 10.10.246.1 source vlan 3248
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 10.10.246.1, timeout is 2 seconds:
```

```
Packet sent with a source address of 10.10.248.1
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/7/8 ms
```

NAT変換が正しく表示されていることを確認します。

```
<#root>
```

```
Router#
```

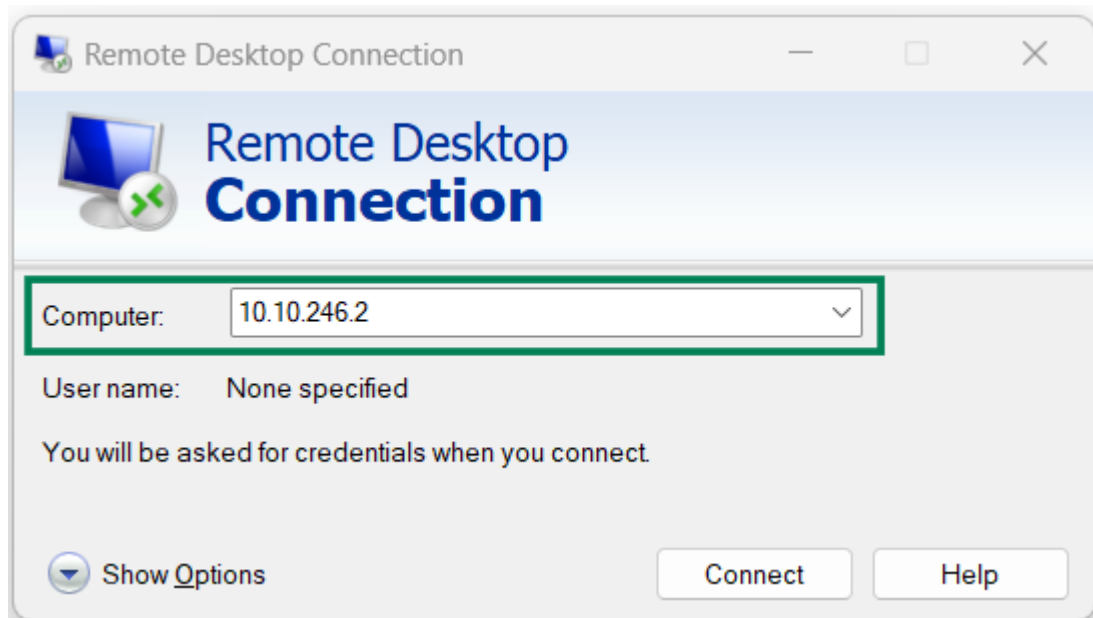
```
show ip nat translations
```

```
Pro Inside global Inside local Outside local Outside global
icmp 10.10.246.2:12 10.10.248.1:12 10.10.246.1:12 10.10.246.1:12
Total number of translations: 1
```

オプションのNAT設定手順を使用する場合は、vLAN3246からvLAN3248のデバイスへのRDP接続が成功していることを確認します。

このドキュメントの例ではRDPを使用していますが、他の任意のプロトコルを使用できます。

ルータで設定されているvLAN3246のSVI(10.10.246.2)を使用して、vLAN3248内のルータの背後にあるデバイス10.10.248.10にRDP接続を行います。



RDPリモートデバイス

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。